Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та кібербезпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

КОРПОРАТИВНА МЕРЕЖА ДП «ЕКСІМА ПЛЮС»

CORPORATE NETWORK SE «EXIMA PLUS»

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІс-21
Пасічніченко Дмитро Олександрович

(підпис)

Керівник:
к.т.н., доцент
Бортник Катерина Яківна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 07 » червня 2024 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2024 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та кібербезпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ проф. Н.Чернящук
« 10 » 01 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Пасічніченку Дмитру Олександровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Корпоративна мережа ДП «Ексіма плюс»*

Керівник роботи *к.т.н., доцент Бортник Катерина Яківна*

затверджені наказом закладу вищої освіти від «30» грудня 2023 року № 459/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 11.06.2024р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, зарубіжні та вітчизняні роботи в даній області, різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Загальні відомості про мережі
Відомості про засоби розробки
Опис розробки корпоративної мережі
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Рішення які були раніше використані
Технології які використовувалися
Вигляд інтерфейсу системи
Архітектура системи

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз проблеми за темою роботи та постановка завдань дослідження	*Бортник К.Я., доцент*		
Теоретичне дослідження та практична реалізація	*Бортник К.Я., доцент*		
Практична реалізація об'єкта проектування	*Бортник К.Я., доцент*		
Нормоконтроль	*Багнюк Н.В., доцент*		
Гарант ОП	*Лавренчук С.В., доцент*		
Показник запозичень тексту	***___%***		
Академічна доброчесність	*Міскевич О.І.,асистент*		

7. Дата видачі завдання 10.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Обгрунтування теми*	до 15.11.2024 р.	Виконано
2.	*Огляд літератури із досліджуваної проблеми*	до 15.12.2024 р.	Виконано
3.	*Теоретична частина*	до 02.02.2024 р.	Виконано
4.	*Опис засобів розробки*	до 02.03.2025 р.	Виконано
5.	*Практична частина*	до 15.04.2025 р	
6.	*Формування списку використаних джерел*	до 20.04.2024 р.	Виконано
7.	*Формування додатків*	до 02.05.2024 р.	Виконано
8.	*Оформлення ілюстративного матеріалу*	до 15.05.2024 р.	Виконано
9.	*Нормоконтроль*	до 01.06.2024 р.	Виконано
10.	*Інструментальна перевірка на академічний плагіат*	до 04.06.2024 р	Виконано
11.	*Представлення кваліфікаційної роботи бакалавра до захисту*	до 18.06.2024 р.	Виконано

Здобувач вищої освіти _____ Пасічніченок Д.О.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Бортник К.Я.
(підпис) (прізвище, ініціали)

АНОТАЦІЇ

Пасічніченко Д.О. Корпоративна мережа ДП «Ексіма плюс».

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2024.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел.

Перший розділ присвячено огляду предметної олбасті, тут розглядаються основні поняття про терміни і поняття, які відіграють важливу роль у розумінні комп'ютерних мереж. Окрім цього, у розділі були представлені різні технології, які використовуються для побудови локальних мереж. Також були розглянуті бездротові технології Wi-Fi, які дозволяють безпроводову передачу даних у межах комп'ютерної мережі.

В другому розділі здійснено вибір та обгронтування засобів розробки.

Третій розділ присвячено розробці корпоративної мережі.

Об'єкт – корпоративні мережі та їх компоненти.

Предмет – алгоритми та протоколи, які використовуються для маршрутизації, комутації та захисту даних у корпоративних мережах.

Метою роботи є створення проекту мережі для підприємства.

Ключові слова: комп'ютерні мережі, протоколи зв'язку, маршрутизація, комутація, сегментація мережі.

ANNOTATION

Pasichnychenko D.O. Corporate Network of «Exima Plus» LLC.

Qualification work for Bachelor's Degree in Computer Engineering, Specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2024.

The qualification work consists of an introduction, three chapters, conclusions, and a list of used sources.

The first chapter is devoted to the subject area overview, where the main concepts and terms essential for understanding computer networks are discussed. Additionally, various technologies used for building local networks were presented in this chapter. Wireless Wi-Fi technologies enabling wireless data transmission within computer networks were also examined.

In the second chapter, the selection and justification of development tools were carried out. Chosen: Cisco software.

The third chapter focuses on the development of a corporate network.

Object – corporate networks and their components.

Subject – algorithms and protocols used for routing, switching, and data protection in corporate networks.

The aim of the work is to create a network project for the enterprise.

Keywords: computer networks, communication protocols, routing, switching, network segmentation

ЗМІСТ

ВСТУП

Актуальність теми. Мережі є життєво важливими для сучасних організацій, оскільки вони забезпечують комунікацію та обмін даними всередині компанії та з зовнішнім світом. Вони є основою для виконання бізнес-процесів, від спілкування між співробітниками до управління ресурсами та клієнтськими відносинами. Розвиток технологій, таких як хмарні обчислення, Інтернет речей (IoT) та штучний інтелект, збільшує складність та важливість корпоративних мереж.

Метою роботи є розробка та аналіз ефективних рішень для створення та управління корпоративними мережами.

Об’єкт дослідження – корпоративні мережі та їх компоненти, включаючи мережеве обладнання, сервери, пристрої кінцевих користувачів та програмне забезпечення, яке забезпечує їх взаємодію та управління.

Предмет дослідження – алгоритми та протоколи, які використовуються для маршрутизації, комутації та захисту даних у корпоративних мережах.

Завдання, які потрібно виконати:

– розробити проект комп’ютерної мережі для підприємства;

– проаналізувати та вибрати найкращі протоколи маршутизації та комутації;

– виконати налаштування мережевого обладнання;

– впровадити засоби безпеки в мережу.

Практичне значення роботи полягає в розробці та впровадженні надійної та захищеної корпоративної мережі, що сприятиме підвищенню ефективності бізнес-процесів та оптимізації управління ресурсами. Безпечна мережа забезпечить стабільну та швидку комунікацію, що покращить продуктивність праці та скоротить затримки у виконанні завдань. Правильний вибір протоколів маршрутизації та комутації, а також налаштування мережевого обладнання забезпечать безперебійну роботу мережі, що покращить технологічний розвиток компанії.

РОЗДІЛ 1
ЗАГАЛЬНІ ВІДОМОСТІ ПРО МЕРЕЖІ

1.1 Основні поняття та історія розвитку мережі

Історія розвитку мереж бере свій початок у стародавні часи, коли люди об'єднувалися для спільної діяльності та обміну інформацією. Від давніх торгових маршрутів до сучасних глобальних мереж, ідея об'єднання людей для обміну ідеями та ресурсами завжди мала велике значення. Проте справжня ера мереж почалася у 19-20 століттях із зародженням телеграфії та телефонії. Перші мережі працювали на аналогових принципах та використовували провідні лінії. Ці досягнення були вражаючими, оскільки вони відкрили можливість віддаленої комунікації на великі відстані.

Прототип глобальної комп'ютерної мережі був описаний в 1960 році Дж. Ліклідером. Проект Ліклідера спрямовувався на створення мережі комп'ютерів без централізованого керування, щоб забезпечити обмін даними між вузлами, що розташовані у різних місцях. Основною метою було забезпечити ефективний обмін інформацією між державними, науковими та академічними установами, які займалися проектами з обробки інформації. Ідея Ліклідера викликала інтерес і у 1960-х роках армія США розробила ARPANET – першу мережу, яка застосовувала технологію комутації пакетів і відіграла ключову роль у створенні основ Інтернету. ARPANET забезпечував комунікацію між науковими установами, які співпрацювали у розробці оборонних технологій. В 1980-х роках ARPANET перетворився на мережу яка була доступна для громадськості.

Початок 1990-х років був відзначений народженням World Wide Web (WWW), що відкрило шлях до найбільшої епохи розвитку інформаційних технологій. У 1991 році Тім Бернерс-Лі, британський фізик, інженер-програміст та винахідник розробив перший браузер WorldWideWeb (пізніше його перейменували на Nexus). Це дозволило користувачам переглядати веб-сторінки,використовуючи гіпертекстові посилання. У 1993 році був випущений перший веб-сервер NCSA Mosaic, який став доступний для широкого загалу та

сприяв поширенню WWW.З’явились перші пошукові системи, такі як Yahoo! та AltaVista, які спростили процес пошуку вмісту в Інтернеті.

Протягом останніх десятиліть розвиток Інтернету та мережевих технологій стрімко просувався вперед. Поява та вдосконалення бездротових технологій, таких як Wi-Fi, дозволили людям з’єднуватися з мережею з будь-якого місця. Сьогодні інтернет перетворився на безмежне джерело інформації, розваг та можливостей для комунікації, що неперервно розвивається та адаптується під впливом нових технологій та потреб користувачів.

Комп’ютерна мережа – це система взаємопов’язаних комп’ютерів та інших пристроїв, яка забезпечує їх комунікацію між собою та забезпечує обмін інформацією та ресурсами.

Основні компоненти будь-якої мережі:

– вузли – це комп’ютери або інші пристрої, які підключені до мережі і можуть надсилати, отримувати або обробляти дані;

– з’єднання – це канали, через які дані передаються між вузлами. Вони можуть бути провідними (Ethernet - кабелі) або безпровідними (Wi-Fi, Bluetooth).

Ethernet-кабелі також відомі, як LAN-кабелі або мережеві кабелі, є фізичними засобами передачі даних для мережевого з’єднання. Вони використовуються для підключення комп’ютерів, маршрутизаторів, комутаторів та інших мережевих пристроїв для обміну даними в мережах Ethernet.

Ethernet-кабелі використовуються для створення провідних мереж, в яких дані передаються за допомогою електричних сигналів по мідним або волоконно-оптичним кабелям. Найпоширенішим типом Ethernet-кабелю є кабель категорії 5e (Cat5e) або кабель категорії 6 (Cat6), які підтримують високу швидкість передачі даних і забезпечують надійне з’єднання.

Ethernet-кабелі мають різні конструкції і конфігурації, такі як прямі (straight-through) кабелі, які використовуються для підключення комп’ютера до маршрутизатора або комутатора, та перехресні (crossover) кабелі, які використовуються для підключення двох пристроїв однакового типу, наприклад, комп’ютера до комп’ютера або маршрутизатора до маршрутизатора.

Ethernet-кабелі можуть мати різні довжини від декількох метрів до кількох сотень метрів, в залежності від потреб мережі. Вони також можуть бути захищені від зовнішніх впливів, таких як волога або електромагнітні перешкоди, що забезпечується захисними оболонками або екранами.

У сучасних мережах Ethernet-кабелі використовуються для побудови провідних мереж різного масштабу, від домашніх мереж до великих корпоративних інфраструктур, що дозволяє ефективно обмінюватися даними і забезпечувати зв'язок між пристроями.

Wi-Fi, або бездротова мережа, – це технологія, яка дозволяє бездротово підключатися до Інтернету або інших пристроїв всередині обмеженої області, яку називають зоною покриття. Слово «Wi-Fi» є товарним знаком і походить від фрази «Wireless Fidelity».

Wi-Fi використовує радіохвилі для передачі даних між пристроями, такими як комп'ютери, смартфони, планшети, смарт-телевізори та інші. Ця технологія базується на стандартах IEEE 802.11, який визначає методи доступу до середовища та протоколи для бездротового зв'язку.

Переваги Wi-Fi включають в себе зручність підключення без проводів, мобільність (користувачі можуть підключатися до мережі всередині зони покриття), а також можливість підключення кількох пристроїв до однієї мережі. Проте Wi-Fi має й деякі недоліки. Наприклад, швидкість передачі даних може бути нижче, ніж у проводних з'єднань, особливо при великій кількості підключених пристроїв або при наявності перешкод у сигналі. Також існує ризик безпеки, пов'язаний з можливістю несанкціонованого доступу до мережі.

У сучасному світі Wi-Fi став неот'ємною частиною повсякденного життя, використовуючись у домашніх мережах, громадських місцях, офісах, аеропортах, кафе та багатьох інших місцях, надаючи людям доступ до Інтернету та обміну даними без проводів.

Bluetooth – це бездротовий протокол зв'язку, розроблений для обміну даними між електронними пристроями на невеликій відстані, зазвичай до 10 метрів. Назва «Bluetooth» походить від давньоскандинавського короля Гаральда

Bluetooth, який єднив народи, що нагадує про спробу цієї технології об’єднати різні типи пристроїв у єдину бездротову мережу.

Bluetooth дозволяє пристроям спілкуватися між собою і обмінюватися різними видами даних, такими як аудіо, відео, текстові повідомлення, контакти та інші. Ця технологія широко використовується в різних пристроях, таких як смартфони, навушники, колонки, клавіатури, миші, автомобільні системи та інші.

Однією з головних переваг Bluetooth є простота встановлення з’єднання між пристроями і можливість автоматичного відновлення з’єднання при знаходженні в зоні дії. Вона також відома своєю енергоефективністю, що дозволяє пристроям працювати на дуже малій кількості енергії, що особливо важливо для портативних пристроїв.

Проте, Bluetooth має обмеження в швидкості передачі даних порівняно з іншими бездротовими технологіями, такими як Wi-Fi. Також він може бути схильний до перешкод у місцях з великою кількістю бездротових пристроїв.

Вцілому, Bluetooth є важливою бездротовою технологією, яка використовується в різних аспектах нашого життя, забезпечуючи зручність і можливості спілкування між пристроями;

– пристрої, до яких відносяться маршрутизатори, комутатори, хаби та інші пристрої, які допомагають направляти трафік у мережі. Вони забезпечують зв’язок між різними вузлами та управління потоками даних.

Маршрутизатор – це пристрій комп’ютерної мережі, який використовується для передачі даних між різними мережами. Основна функція маршрутизатора полягає в прийомі, обробці та направленні даних між мережевими пристроями.

Маршрутизатори використовуються в різних мережевих середовищах, включаючи домашні мережі, малий бізнес, великі корпорації та Інтернет-провайдерів. Вони є ключовими складовими мережевої інфраструктури, які забезпечують ефективний обмін даними між різними пристроями та мережами.

Основні функції маршрутизаторів:

– маршрутизація. Прийом, обробка та направлення пакетів даних між різними мережами;

– qos (quality of service). Управління пропускною здатністю та пріорите тами для різних типів трафіку;

– переключення портів. Можливість підключення різних мережних пристроїв через різні порти маршрутизатора;

– dhcp. Надання IP-адрес та інших мережних налаштувань автоматично пристроям у мережі;

– мережевий тунель. Забезпечення безпечного з'єднання між віддаленими мережами через Інтернет.

Комутатор – це пристрій комп'ютерної мережі, який використовується для підключення різних мережних пристроїв і передачі даних між ними в мережі Ethernet. Основна функція комутатора полягає в пересиланні пакетів даних з одного пристрою до іншого в мережі, забезпечуючи швидку та ефективну передачу.

Основні функції комутаторів:

– пересилання кадрів даних. Комутатор приймає пакети даних на одному порту і пересилає їх на відповідний порт, на якому знаходиться призначений пристрій, забезпечуючи ефективну передачу даних;

– розділення на VLAN. Створює логічні групи пристроїв у мережі (VLAN), що дозволяє керувати трафіком і забезпечувати безпеку;

– безпека мережі. Надає різні засоби захисту мережі, включаючи контроль доступу до портів, виявлення аномальних ситуацій та блокування шкідливого трафіку;

– журналювання подій. Записує інформацію про події і стан мережі для аналізу та відновлення після виникнення проблем.

Хаб – це пристрій комп'ютерної мережі, який дозволяє підключати різні мережні пристрої і передавати дані між ними. Основна функція хаба полягає в

розподілі даних, які надходять на один порт, на всі інші порти, що дозволяє пристроям у мережі обмінюватися інформацією. Хаби були популярні в ранній епохи розвитку мережевих технологій, але зараз вони переважно витіснені комутаторами, які забезпечують більшу швидкість передачі даних, меншу ймовірність колізій та більшу ефективність мережі в цілому. Однак деякі хаби все ще використовуються в специфічних випадках, наприклад, для створення дешевих мереж або тестування мережного з'єднання.

Топологія комп'ютерної мережі визначає спосіб, яким з'єднані комп'ютери та інші пристрої в мережі. Основні типи топологій комп'ютерних мереж:

– зірка (рисунок 1.1). У цій топології кожен комп'ютер підключений безпосередньо до центрального вузла, який може бути комутатором або концентратором. Вся комунікація між комп'ютерами відбувається через центральний вузол. Це дозволяє легко додавати або видаляти пристрої, а також забезпечує надійність мережі;

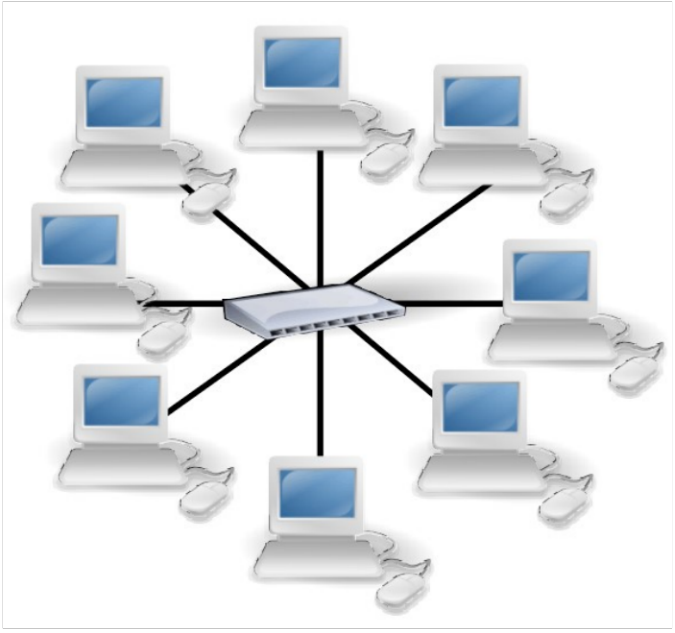

Рисунок 1.1 – Приклад топології «Зірка» [6]

– кільце (рисунок 1.2). У кільцевій топології кожен вузол з'єднаний з двома сусідніми вузлами, утворюючи замкнений кільцевий шлях. Дані пересилаються

по кільцю в одному напрямку. Коли один вузол надсилає дані, вони проходять через кожен вузол на шляху до призначеного вузла.

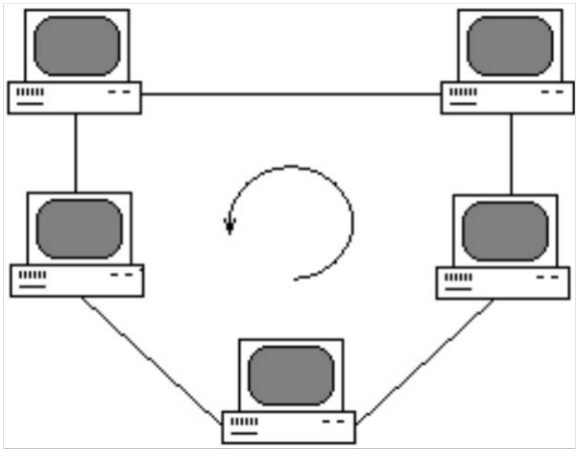

Рисунок 1.2 – Приклад топології «Кільце» [8]

Кільцева топологія досить надійна, але в разі відмови одного вузла вся мережа може перестати працювати;

– шина (рисунок 1.3). У цій топології всі пристрої підключені до одного спільного кабелю, який називається шиною або магістраллю. Кожен пристрій має доступ до цього кабелю і може спілкуватися з іншими пристроями, використовуючи нього. Шина може бути вразливою до перешкод або відмов, що може призвести до втрати зв’язку;

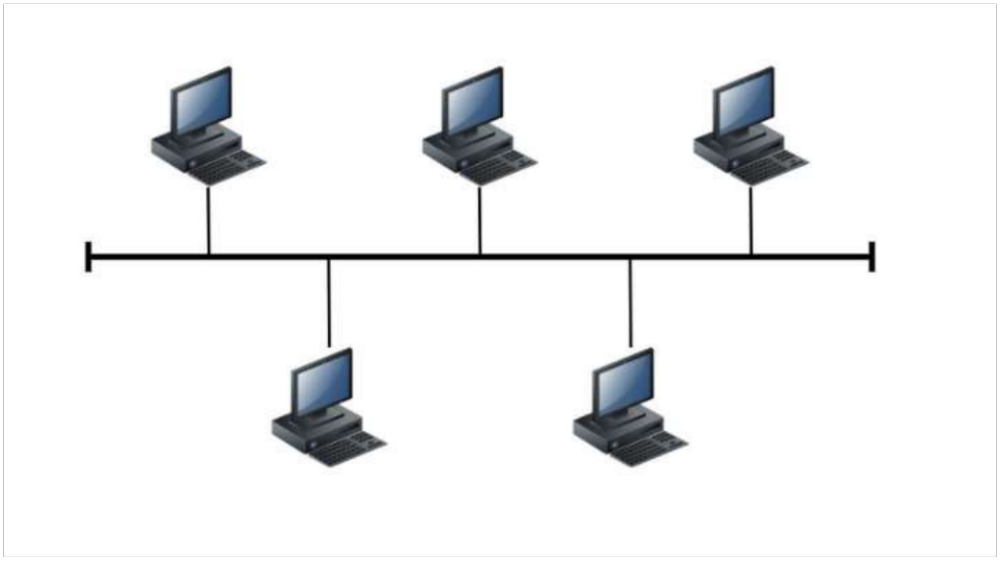

Рисунок 1.3 – Приклад топології «Шина» [9]

– дерево (рисунок 1.4). Топологія дерева включає в себе комбінацію зіркових мереж, які об’єднані в одну загальну мережу. Наприклад, може бути кілька зіркових мереж, кожна з яких має свій центральний вузол, і ці центральні вузли можуть бути підключені до центрального вузла ще вищого рівня;

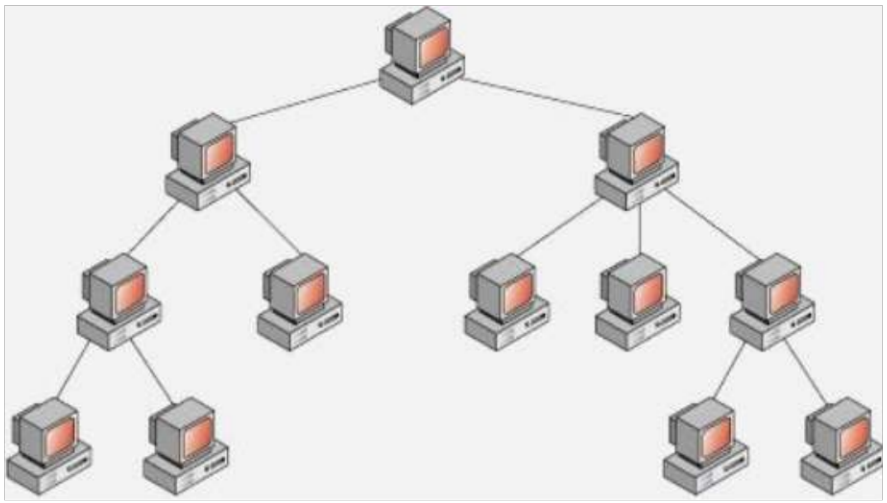

Рисунок 1.4 – Приклад топології «Дерево» [5]

– меш (рисунок 1.5). В меш-мережах кожен пристрій має з’єднання з кожним іншим пристроєм у мережі. Це забезпечує велику надійність та широку пропускну здатність, але вимагає значних ресурсів для розгортання та управління.

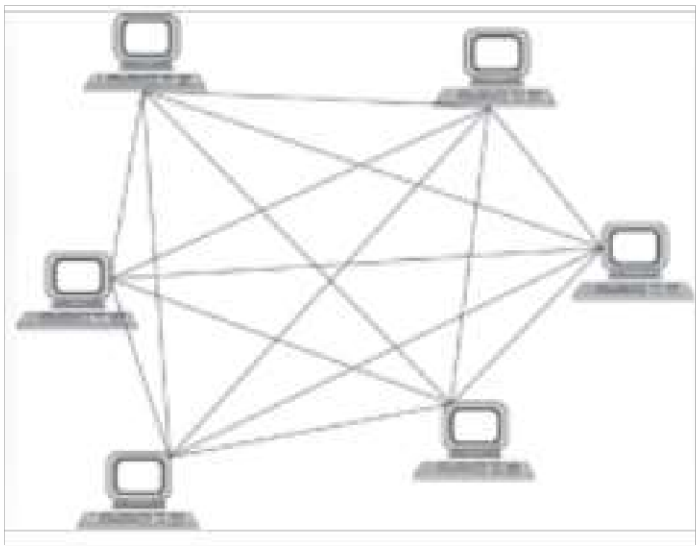

Рисунок 1.5 – Приклад топології «Меш» [7]

1.2 Типи мереж та основні стандарти та протоколи

Мережеві протоколи – це набір стандартів та правил, які визначають, як пристрої в мережі обмінюються даними та взаємодіють один з одним. Ці протоколи дозволяють різним пристроям та програмам спілкуватися між собою та виконувати різноманітні завдання в мережевому середовищі. Ось кілька основних мережевих протоколів:

– tcp/ip (transmission control protocol/internet protocol). Цей набір протоколів складається з двох основних частин: TCP і IP. TCP (Transmission Control Protocol) - надійний протокол забезпечення транспортного рівня, який гарантує доставку даних в порядку, в якому вони були відправлені, та перевіряє їх цілісність. TCP використовується для передачі даних, які вимагають надійної доставки, таких як веб-сторінки, електронна пошта, файли тощо. IP (Internet Protocol) - протокол мережевого рівня, який відповідає за маршрутизацію пакетів даних в мережі. IP визначає, як адресувати та передавати дані між вузлами мережі;

– udp (user datagram protocol). Це протокол, який працює на тому ж рівні, що й TCP, але не гарантує надійну доставку даних. Він використовується там, де невелика затримка важливіша, ніж надійність, наприклад, в потокових мультимедійних додатках;

– http (jypertext transfer protocol). Цей протокол використовується для передачі веб-сторінок між веб-серверами та веб-браузерами. HTTP використовується для отримання статичного вмісту, такого як HTML-сторінки, з сервера;

– ftp (file transfer protocol). Цей протокол використовується для передачі файлів між комп’ютерами в мережі. Він дозволяє користувачам керувати файлами на віддаленому сервері, виконуючи операції, такі як завантаження та вивантаження файлів;

– smtp (simple mail transfer protocol). Цей протокол використовується для відправки електронної пошти між серверами електронної пошти. Він дозволяє передавати повідомлення електронної пошти від одного сервера до іншого;

– pop 3 (post office protocol version 3) та imap (internet message access protocol). Ці протоколи використовуються для отримання електронної пошти з сервера на клієнтському пристрої. POP3 завантажує повідомлення із сервера та видаляє їх, тоді як IMAP синхронізує клієнтський пристрій з поштовим сервером, зберігаючи повідомлення на сервері.

Модель OSI (Open Systems Interconnection) - це концептуальна модель (рисунок 1.6), яка була розроблена Міжнародною організацією зі стандартизації (ISO) з метою стандартизації та опису функцій комп'ютерних мереж та комунікаційних систем.

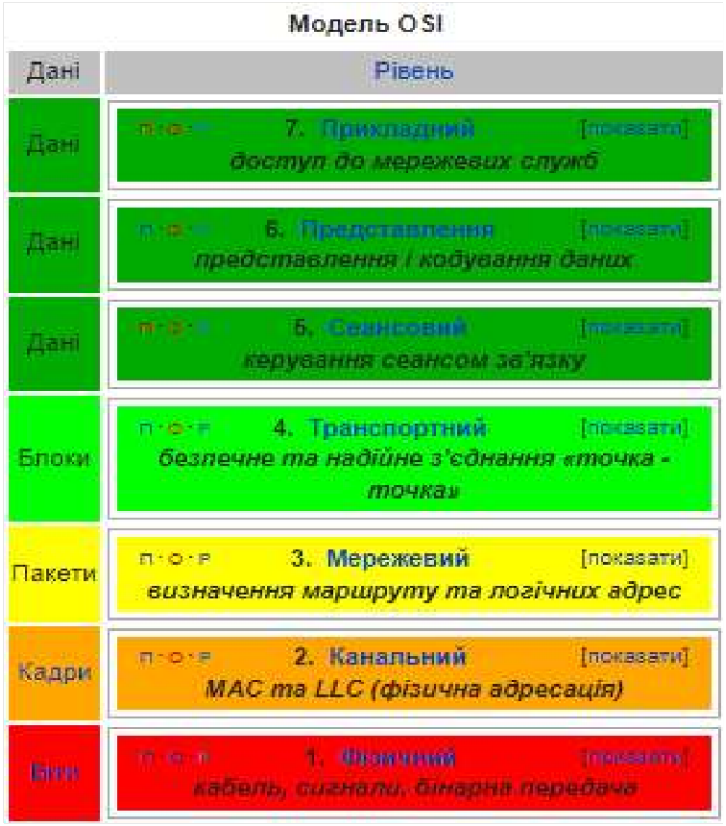

Рисунок 1.6 – Вигдяд моделі OSI [3]

Модель OSI розділяє процес передачі даних на сім логічних рівнів, кожен з яких виконує певні функції. Короткий опис кожного з рівнів:

– фізичний рівень (physical layer). Цей рівень відповідає за передачу нулів та одиниць через фізичні медіа, такі як мідь, оптика або бездротові канали;

– канальний рівень (data link layer). Канальний рівень відповідає за забезпечення надійного з'єднання між пристроями на фізичному рівні та керує передачею даних у рамках одного фізичного зв'язку;

– мережевий рівень (network layer). Цей рівень керує маршрутизацією даних у мережі, визначає найкращий шлях для передачі даних від вихідного вузла до призначеного вузла;

– транспортний рівень (transport layer). Транспортний рівень забезпечує надійність доставки даних та керує потоками даних між вузлами;

– сеансовий рівень (session layer). Цей рівень встановлює, управляє та завершує сеанси зв'язку між пристроями;

– представницький (presentation layer). Представницький рівень забезпечує перетворення даних у сприйнятний для користувача формат та керує синтаксичним та семантичним зрозумінням даних;

– прикладний рівень (application layer). Прикладний рівень надає інтерфейс для взаємодії користувача з мережевими послугами та додатками.

Інститут інженерів електротехніки та електроніки (IEEE) є однією з провідних міжнародних організацій, яка розробляє стандарти в галузі електротехніки, електроніки та пов'язаних технологій. Стандарти IEEE широко використовуються у всьому світі для забезпечення сумісності, інтероперабельності та якості в різних сферах.

Найвідоміші стандарти IEEE:

– ieee 802.11 (wi-fi). Цей стандарт визначає характеристики бездротових локальних мереж (WLAN). Він охоплює різні версії, такі як 802.11a(Швидкість передачі даних: до 54 Мбіт/с.), 802.11b(Швидкість передачі даних: до 11 Мбіт/с.), 802.11g(Швидкість передачі даних: до 54 Мбіт/с.), 802.11n(Швидкість передачі даних: до 600 Мбіт/с (теоретично).), 802.11ac(Швидкість передачі даних: до 3.47

Гбіт/с (теоретично).) та 802.11ax(Швидкість передачі даних: до 9.6 Гбіт/с (теоретично).), і встановлює правила для передачі даних через бездротові канали;

– ieee 802.3 (ethernet). Цей стандарт визначає характеристики проводових локальних мереж (LAN) та передачі даних через Ethernet-кабелі. Він охоплює різні типи Ethernet, включаючи 10BASE-T(Швидкість передачі даних:10 Мбіт/с.), 100BASE-TX(Швидкість передачі даних: 100 Мбіт/с.), 1000BASE-T(Швидкість передачі даних: 1 Гбіт/с.);

– ieee 802.15 (Bluetooth). Цей стандарт визначає характеристики персональних бездротових мереж (WPAN), зокрема технології Bluetooth;

– ieee 754 (Floating Point Arithmetic). Цей стандарт визначає формати чисел з плаваючою комою та арифметичні операції для їх обробки в комп'ютерних системах;

– ieee 1394 (FireWire). Цей стандарт визначає характеристики високошвидкісного інтерфейсу передачі даних, який використовується для підключення пристроїв, таких як відеокамери, зовнішні жорсткі диски тощо.

Це лише кілька прикладів стандартів IEEE, існують також багато інших стандартів, які охоплюють широкий спектр технологій та застосувань. Ці стандарти сприяють розвитку та стандартизації технологічних рішень у всьому світі.

Комп'ютерні мережі можна класифікувати за різними критеріями, такими як розмір, топологія, тип зв'язку та призначення. Ось деякі типи комп'ютерних мереж, які часто зустрічаються:

1. За розміром:

– локальні мережі (lan). Охоплюють обмежену територію, таку як офіс, кампус, будинок або заводський комплекс. Вони зазвичай використовуються для з'єднання комп'ютерів та інших пристроїв у межах одного місця для обміну даними та ресурсами.. Приклад використання - використовуються в офісах для спільного використання принтерів, сховищ даних, доступу до Інтернету та обміну інформацією між працівниками;

– міські мережі (man). MAN охоплюють більшу територію, таку як ціле місто або регіон. Вони зазвичай складаються з кількох LAN, які підключені один до одного. Міські мережі використовуються телекомунікаційними компаніями для підключення локальних мереж, мереж великих корпорацій або установ, а також для надання послуг доступу до Інтернету в місті;

– глобальні мережі (wan). WAN охоплюють великі географічні області, такі як країни, континенти або навіть весь світ. Вони складаються з набору MAN та інших мережних сегментів, підключених за допомогою мережевого обладнання та телекомунікаційних ліній. Глобальні мережі, такі як Інтернет, використовуються для забезпечення спілкування, доступу до інформації та ресурсів для користувачів у всьому світі. Крім того, багато міжнародних компаній використовують WAN для забезпечення спільного використання даних та ресурсів між своїми віддаленими офісами та філіями.

2. За топологією:

– зіркова топологія;

– кільцева топологія;

– шинна топологія;

– меш-топологія.

3. За типом зв’язку:

– провідна мережа. Використовує фізичні кабелі для передачі даних;

– бездротова мережа. Використовує радіохвилі для передачі даних між пристроями.

4. За призначенням:

– бізнес-мережа. Використовується у бізнес-середовищах для обміну даними, спільного використання ресурсів та спілкування;

– домашня мережа. Використовується в домашньому середовищі для спільного використання Інтернету, друку, файлів тощо;

– навчальна мережа. Використовується в освітніх закладах для навчання, обміну інформацією та ресурсами.

1.3 Архітектура мережі

Архітектура мережі є важливим елементом проектування мережі, що визначає її структуру, компоненти та взаємозв'язки між ними.

Основні компоненти мережевої архітектури:

– клієнтські пристрої. Пристрої, які використовуються співробітниками для доступу до мережевих ресурсів (комп'ютери, ноутбуки, смартфони, планшети);

– мережеве обладнання. Комутатори відповідають за комутацію даних у локальній мережі . Забезпечують високошвидкісне з'єднання між клієнтськими пристроями та серверами; маршрутизатори використовуються для з'єднання різних мереж та управління трафіком між ними. Маршрутизатори також забезпечують підключення до Інтернету; точки доступу забезпечують бездротовий доступ до мережі для мобільних пристроїв;

– сервери. Файлові сервери призначені для зберігання та управління файлами; сервери додатків використовують для роботи корпоративних додатків; сервери баз даних застосовуються для зберігання та обробки даних підпри ємства; контролери домену керують доступом та автентифікацією користувачів;

– засоби забезпечення безпеки. Міжмережеві екрани захищають мережу від несанкціонованого доступу та кіберзагроз; системи запобігання вторгненням виявляють та запобігають атакам на мережу; VPN шлюзи забезпечують безпечний віддалений доступ до мережі.

Логічна структура мережі:

– класифікація підмереж. Керуюча мережа виділена для управління мережевим обладнанням та серверами; корпоративна мережа – це основна мережа для роботи співробітників; гостьова мережа призначена для відвідувачів підприємства з обмеженим доступом до ресурсів;

– віртуалізація мережевих функцій. Використання програмних рішень для реалізації мережевих функцій, які знижують залежність від апаратного забезпечення та підвищують гнучкість управління мережею;

– поділ мережі на сегменти VLAN. Поділ фізичної мережі на логічні сегменти дозволяє підвищити безпеку та ефективность управління трафіком.

Фізична структура мережі:

– централізована архітектура. Використання одного або декількох центральних комутаторів для з’єднання всіх підмереж;

– ієрархічна архітектура. Центральний рівень використовується для високошвидкісного з’єднання та маршрутизації між підмережами; проміжний рівень використовують для агрегації трафіку від кількох підмереж та застосування політик безпеки; рівень доступу, на ньому з’єднуються кінцеві пристрої з мережею;

– розташування обладнання. Дата-центри відповідають за централізоване зберігання та обробку даних; комунікаційні шафи – це локальне розміщення мережевого обладнання для певних відділів або будівель.

Високодоступність та відмовостійкість:

– резервування. Застосування резервних каналів зв’язку та обладнання для забезпечення безперервної роботи мережі;

– відмовостійкість. Запровадження механізмів автоматичного віднов лення після збоїв.

РОЗДІЛ 2
ЗАГАЛЬНІ ВІДОМОСТІ ПРО ЗАСОБИ РОЗРОБКИ

2.1 Програмне забезпечення

Cisco Packet Tracer – це інтерактивна платформа для моделювання мережевих систем та експериментів з їх конфігурацією. Вона розроблена спеціально для студентів і фахівців з мережевих технологій, щоб надати їм можливість вивчати, тестувати та експериментувати з різними аспектами мережевого з'єднання.

Основні переваги:

– інтуїтивний інтерфейс. Простий у використанні графічний інтерфейс, який дозволяє швидко створювати мережеві топології;

– широкий набір інструментів. Наявність різноманітних мережевих пристроїв, таких як комутатори, маршрутизатори, точки доступу, сервери та клієнтські пристрої;

– підтримка протоколів. Підтримка основних мережевих протоколів, таких як TCP/IP, OSPF, EIGRP, VLAN, NAT, та інших;

– навчальні можливості. Інструмент активно використовується в навчальних закладах для підготовки мережевих фахівців.

Основні функції Cisco Packet Tracer:

– моделювання мереж. Packet Tracer дозволяє створювати віртуальні мережі, які складаються з різних мережевих пристроїв, таких як маршрутиза тори, комутатори, комп'ютери, сервери тощо;

– конфігурація пристроїв. Користувачі можуть конфігурувати параметри кожного пристрою, такі як IP-адреси, маршрути, VLAN тощо, і вивчати взаємодію між ними;

– симуляція мережевих процесів. Packet Tracer надає можливість спостерігати за тим, як дані передаються через мережу, як працює маршру

тизація, комутація, а також як відбувається виявлення і усунення несправ ностей;

– навчальні ресурси. Містить різноманітні навчальні матеріали, такі як лабораторні роботи, практичні завдання та вправи, що допомагають у засвоєнні мережевих концепцій та протоколів;

– співпраця та обмін проектами.-Packet Tracer дозволяє користувачам обмінюватися своїми мережевими проектами, а також співпрацювати над ними в реальному часі.

Cisco Packet Tracer є важливим інструментом для навчання та розвитку навичок у галузі мережевих технологій з кількох причин:

– практичне навчання. Packet Tracer дозволяє студентам отримувати практичний досвід роботи з мережевими пристроями, будуючи віртуальні мережі та конфігуруючи їх. Це дозволяє їм краще зрозуміти теоретичні концепції через практичні застосування;

– експериментація без ризику. Packet Tracer дозволяє студентам експериментувати з різними конфігураціями мережі без ризику збоїв чи втрати даних в реальному середовищі. Це створює безпечне середовище для вивчення й вдосконалення навичок;

– візуалізація концепцій. Використання Packet Tracer дозволяє студентам візуалізувати мережеві концепції та процеси, що допомагає в їх кращому розумінні. Вони можуть спостерігати за тим, як дані переміщуються через мережу та як працюють різні мережеві пристрої;

– співпраця та обмін досвідом. Packet Tracer також дозволяє студентам співпрацювати над проектами та обмінюватися досвідом з колегами. Це створює можливість для взаємного навчання та вирішення складних завдань разом;

– підготовка до сертифікацій. Для тих, хто готується до сертифікаційних іспитів у галузі мережевих технологій, Packet Tracer може бути корисним інструментом для практичної підготовки, дозволяючи засвоювати матеріал і виконувати практичні завдання, які часто зустрічаються на іспитах.

Cisco Packet Tracer також має деякі можливості щодо інтеграції з Інтернетом речей (IoT) та моделювання цих систем. Ось деякі з них:

– моделювання пристроїв IoT. Packet Tracer містить бібліотеку різноманітних пристроїв IoT, таких як датчики, актуатори, мікроконтролери тощо. Користувачі можуть використовувати ці пристрої для створення складних систем IoT в мережевому середовищі;

– протоколи та стандарти IoT. Packet Tracer підтримує різноманітні протоколи і стандарти, які використовуються в інтернеті речей, такі як MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), HTTP, і багато інших. Це дозволяє користувачам вивчати та експериментувати з різними аспектами комунікації в мережі IoT;

– інтеграція з хмарними сервісами. Packet Tracer може бути інтегрований з хмарними сервісами, що дозволяє користувачам спрощено зберігати, обробляти та аналізувати дані, отримані від пристроїв IoT у віртуальних мережах;

– моделювання розумних систем. За допомогою Packet Tracer користувачі можуть моделювати різноманітні розумні системи, такі як системи освітлення, системи безпеки, системи управління енергоефективністю тощо, що базуються на інтернеті речей;

– навчання та дослідження. Packet Tracer надає можливість навчатися та досліджувати концепції та технології IoT в безпечному віртуальному середовищі, що дозволяє експериментувати з різними сценаріями без реальних витрат чи ризику.

Cisco Packet Tracer надає широку підтримку різноманітного мережевого обладнання та протоколів, що дозволяє користувачам ефективно вивчати та експериментувати з різними технологіями. Ось кілька прикладів цієї підтримки:

– мережеве обладнання. Packet Tracer включає в себе широкий спектр мережевого обладнання, такий як маршрутизатори, комутатори, файрволи, маршрутизатори з технологією NAT, DHCP-сервери, мережеві принтери тощо.

Це дозволяє користувачам побудувати різнорівневі мережі та експериментувати з різними архітектурами мереж;

– протоколи мережі. Packet Tracer підтримує широкий спектр мережевих протоколів, включаючи TCP/IP, IPv4, IPv6, OSPF, EIGRP, RIP, BGP, VLAN, DHCP, DNS, SNMP, HTTP, HTTPS, SSH, Telnet та багато інших. Це дозволяє користувачам вивчати та експериментувати з різними аспектами мережевої комунікації та маршрутизації;

– інтеграція з сервісами. Packet Tracer також підтримує інтеграцію з різноманітними мережевими сервісами, такими як DHCP, DNS, TFTP, HTTP, HTTPS, FTP тощо. Це дозволяє користувачам налаштовувати та тестувати різні мережеві сервіси та додаткові функції;

– моделювання безпеки. Packet Tracer також включає в себе можливості моделювання мережевої безпеки, включаючи файрволи, VPN, ACL, IPS, IDS та інші засоби захисту. Це дозволяє користувачам експериментувати з різними методами захисту мережі в безпечному середовищі.

2.2 Апаратне забезпечення

Cisco є відомим виробником мережевого обладнання, і їх продукти використовуються по всьому світу. Основні категорії апаратного забезпечення Cisco:

– маршрутизатори. Cisco ISR (Integrated Services Routers) серія цих маршрутизаторів призначена для малих та середніх підприємств. Вони забезпечують базові послуги, такі як маршрутизація, комутація, безпека, VPN, QoS та інші. Маршрутизатори цієї серії використовуватися як центральні вузли в мережі, об’єднуючи різні підмережі та надаючи доступ до Інтернету. Cisco ASR (Aggregation Services Routers) дана серія підходить для великих підприємств та провайдерів. Вони забезпечують високу пропускну здатність, надійність та масштабованість.ASR-маршрутизатори найчастіше застосовуються в мережах з великим обсягом трафіку;

– комутатори. Cisco Catalyst Series серія комутаторів яка найчастіше використовується в підприємствах. Вона включає в себе широкий спектр моделей, які відрізняються за функціональністю та продуктивністю. Базові моделі призначені для невеликих мереж і мають базовий набір функцій. Середнього класу моделі мають розширений набір можливостей, а саме керування VLAN, QoS, безпека та інші. Високопродуктивні моделі призначені для великих підприємств і вражають своєю швидкістю, можливістю масштабування та рівнем безпеки. Серію комутаорів Cisco Nexus Series використовують в дата-центрах. Вона забезпечує високу продуктивність, надійність та масштабованість. Серія маршрутизаторів Cisco Nexus 3000 була спеціально розроблена для високопродуктивних дата-центрів. Вони мають низьку латентність, що дозволяє забезпечити швидку обробку мережевого трафіку. Ці маршрутизатори ідеально підходять для обробки даних у дата-центрах задовольняючи сучасні вимоги;

– бездротові точки. Cisco Aironet Access Points включає в себе високопродуктивні бездротові точки доступу, які призначені для підприємств. Вони забезпечують надійну бездротову мережу з високою швидкістю передачі даних та підтримкою сучасних стандартів Wi-Fi, таких як Wi-Fi 6. Такі точки доступу найчастіше вибирають для офісів, готелей, магазинів та інших комерційних приміщеннях. Cisco Meraki пропонує хмарні керовані рішення для мереж, включаючи бездротові точки доступу, комутатори та мережеві пристрої безпеки. В цій платформі налаштовування та керування мережею здійснюється через хмару, що спрощує завдання адміністраторам. Крім того, Cisco Meraki надає інтегровані рішення для забезпечення безпеки, що дозволяє об’єднати фізичний захист і кібербезпеку;

– сервери. Cisco UCS (Unified Computing System) є інтегрованою обчислювальною інфраструктурою з управлінням на основі намірів, що автоматизує та прискорює розгортання всіх потрібних додатків. Вона включає в себе обчислювальні ресурси, мережу, віртуалізацію, доступ до сховища даних та програмне забезпечення. Cisco UCS може працювати з різними навантаженнями,

включаючи віртуалізовані та хмарні обчислення, аналітику в пам'яті та роботу на краю мережі. Cisco HyperFlex – це система, що об'єднує комп'ютери, зберігання та мережеві функції в одному місці. Вона дозволяє легко керувати всіма цими ресурсами і забезпечує безпеку. Це, як великий «розумний» сервер, який можна налаштовувати та використовувати для різних завдань. Поєднує в собі властивості хмари з перевагами інфраструктури на місці. Cisco HyperFlex підтримує різноманітні додатки та робочі навантаження такі, як віртуальні робочі столи, віртуалізацію серверів, тестування та розробку;

– безпека. Cisco ASA (Adaptive Security Appliances) є відомим брандмауером, який забезпечує багаторівневий захист мережі. Використовуються для контролю доступу, фільтрації трафіку та виявлення загроз. Cisco ASA має інтегровані можливості IPS, VPN та Unified Communications. Ці пристрої допомагають організаціям покращити продуктивність за допомогою кластерів з високою продуктивністю та багатосайтових мереж. Cisco Firepower надає комплексні рішення для мережевої безпеки. Серія включає в себе NGFW (Next-Generation Firewall), який отримав високі показники ефективності безпеки в сторонніх тестуваннях для якості виявлення загроз. Також вона включає IPS, які блокують загрози на рівні мережі. Cisco Firepower забезпечує контроль над додатками, виявлення загроз та захист від вірусів;

– IP-телефонія та відеоконференції. Cisco Unified Communications – це рішення для корпоративної IP-телефонії. Воно об'єднує різні інструменти співпраці, такі як IP-телефонія для голосового зв'язку, веб- та відеоконференції, голосова пошта, мобільність, обмін робочими столами та миттєві повідомлення. Це дозволяє співробітникам ефективно спілкуватися в межах організації та за її межами. Cisco Webex – це інструмент для відеоконференцій і командної роботи. Він надає можливість проводити безпечні відеоконференції, спільно працювати над проектами та обмінюватися ідеями. Webex також забезпечує високоякісний аудіо та HD-відео зв'язок, легке спільне використання екрану, можливість бачити до 25 учасників одночасно та потужні інструменти для контролю. Це допомагає підвищити продуктивність та покращити співпрацю в команді. Webex

підтримує інтеграцію з різними інструментами та платформами, що робить його гнучким і зручним для використання. Зручний інтерфейс та можливість швидкого налаштування дозволять легко адаптувати даний інструмент до потреб будь-якої організації.

РОЗДІЛ 3
РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Вимоги до мережі

В даному підрозділі описані основні вимоги по проектуванню мережі:

– використовувати ієратичну модель, для забезпечення резервування на кожному рівні. Для забезпечення резервування використовувати два маршрутизатори та два багаторівневі комутатори;

– в кожному відділі має бути бездротова мережу для користувачів;

– в кожного відділу має бути свій VLAN та своя підмережа;

– мережа компанії підключена до статичних загальнодоступних IP-адрес 195.130.8.0/30, 195.130.8.4/30, наданих Інтернет-провайдером;

– мають бути налаштовані основні параметри пристроїв, а саме банерні повідомлення, імена хостів,вимкнений пошук домену IP,пароль консолі та імена хостів;

– пристрої всіх відділів повинні мати змогу комунікувати один з одним за допомогою багаторівневих комутаторів, налаштованих для маршрутизації між VLAN;

– багаторіневі комутатори мають виконувати функціїї комутації та маршрутизації, також їм мають бути призначені IP-адреси;

– всі пристрої мережі отримують IP-адресу динамічно від DHCP сервера розташованого в серверній;

– в серверній кімнаті пристроям IP-адреси присвоюються статично;

– протокол OSPF використовується для маршрутизації та оголошення маршрутів на багаторівневих комутаторах та маршрутизаторах;

– для віддаленого входу необхідно налаштувати SSH на всіх комутаторах третього рівня і маршрутизаторах;

– для відділу фінансів налаштувати безпеку порту так, щоб лише один пристрій міг підключатися до порту комутатора;

– налаштувати PAT, щоб можна було використовувати IPv4-адресу на інтерфейсі вихідного маршрутизатора і додати відповідне правило в ACL.

3.2 Топологія мережі

Для стоворення даної комп’ютерної мережі я вирішив використати топологію змішаного типу. В ній поєднано елементи кількох типів мережевих топологій:

– зірка. Всі пристрої в кожній VLAN (10, 20, 30, 40, 50) підключені до центрального комутатора;

– ієрархічна структура. Мережа має кілька рівнів підключень, де комутатори та маршрутизатори організовані у певній ієрархічній структурі. Два Multilayer Switch виступають в ролі центральних вузлів мережі та використовуються для з’єднання підереж і VLAN;

Причини вибору такої топології:

– продуктивність. Ієрархічна топологія дозволяє ефективно розподіляти трафік між різними рівнями мережі, забезпечуючи високу продуктивність та мінімальні затримки;

– масштабованість. Легкість додавання нових пристроїв та підмереж без впливу на існуючу інфраструктуру;

– відмовостійкість. Резервні з’єднання та пристрої на кожному рівні мережі забезпечують безперебійність роботи навіть у випадку відмови окремих компонентів;

– безпека. Можливість впровадження політик безпеки на різних рівнях мережі, забезпечуючи багатошаровий захист.

Ієрархічна топологія мережі – це спосіб організації комп’ютерних пристроїв та зв’язків між ними. Вона дозволяє створити ефективну, масштабовану та надійну мережу для підприємства. При правильному виборі

обладнання вона зможе забезпечити високу продуктивність, безпеку та стійкість мережі.

3.3 Проектування мережі

Для реалізації проекту в Cisco Packet Tracer були виконані наступні кроки:

– створення мережевої топології. Розміщення комутаторів, маршрутизаторів, точок доступу та серверів відповідно до проектної схеми;

– налаштування VLAN. Створення та конфігурація VLAN для сегментації мережі;

– налаштування маршрутизації. Впровадження протоколів динамічної маршрутизації для забезпечення ефективного маршрутизації трафіку;

– впровадження політик безпеки. Налаштування міжмережевих екранів, VPN та інших засобів безпеки;

– тестування та відлагодження. Виконання симуляції мережевих процесів для перевірки працездатності.

Компанія буде розташовуватись на 3 поверхах:

– перший поверх. Відділ «Продажі та маркетинг» (таблиця 3.1) та «Кадри і логістика» (таблиця 3.2);

– другий поверх. Відділ «Фінанси» (таблиця 3.3) та «Адміністратори» (таблиця 3.4);

– третій. Відділ «ІСТ» (таблиця 3.5) та серверна кімната (таблиця 3.6).

Таблиця 3.1–Таблиця маршрутизації відділу «Продажі і маркетинг»

VLAN	10
Адреса мережі	172.17.1.0
Маска мережі	255.255.255.192
Префікс мережі	/26
Адреса першого вузла	172.17.1.1
Адреса останнього вузла	172.17.1.62
Широкомовна адреса	172.17.1.63
Кількість вузлів мережі	62

Таблиця 3.2 –Таблиця маршрутизації відділу «Кадри і логістика»

VLAN	20
Адреса мережі	172.17.1.64
Маска мережі	255.255.255.192
Префікс мережі	/26
Адреса першого вузла	172.17.1.65
Адреса останнього вузла	172.17.1.126
Широкомовна адреса	172.17.1.127
Кількість вузлів мережі	62

Таблиця 3.3 –Таблиця маршрутизації відділу «Фінанси»

VLAN	30
Адреса мережі	172.17.2.0
Маска мережі	255.255.255.192
Префікс мережі	/26
Адреса першого вузла	172.17.2.1
Адреса останнього вузла	172.17.2.62
Широкомовна адреса	172.17.2.63
Кількість вузлів мережі	62

Таблиця 3.4 –Таблиця маршрутизації відділу «Адміністратори»

VLAN	40
Адреса мережі	172.17.2.64
Маска мережі	255.255.255.192
Префікс мережі	/26
Адреса першого вузла	172.17.2.65
Адреса останнього вузла	172.17.2.126
Широкомовна адреса	172.17.2.127
Кількість вузлів мережі	62

Таблиця 3.5 –Таблиця маршрутизації відділу «ІСТ»

VLAN	50
Адреса мережі	172.17.3.0
Маска мережі	255.255.255.192
Префікс мережі	/26
Адреса першого вузла	172.17.3.1
Адреса останнього вузла	172.17.3.62
Широкомовна адреса	172.17.3.63
Кількість вузлів мережі	62

Таблиця 3.6 – Таблиця маршрутизації серверної кімнати

VLAN	60
Адреса мережі	172.17.3.64

Продовження таблиці 3.6

Маска мережі	255.255.255.248
Префікс мережі	/29
Адреса першого вузла	172.17.3.65
Адреса останнього вузла	172.17.3.70
Широкомовна адреса	172.17.3.71
Кількість вузлів мережі	6

З’єднання між роутерами R1 і R2 та MLSW1 І MLSW2(таблиця 3.7 – 3.10)

Таблиця 3.7 – Маршрутизація R1 - MLSW1

З’єднання	R1 - MLSW1
Адреса мережі	172.17.3.72
Маска підмережі	255.255.255.252
Префікс мережі	/30
Адреса першого вузла	172.17.3.73
Адреса останнього вузла	172.17.3.74
Широкомовна адреса	172.17.3.75
Кількість вузлів мережі	2

Таблиця 3.8 – Маршрутизація R1 – MLSW2

З’єднання	R1 – MLSW2
Адреса мережі	172.17.3.76
Маска підмережі	255.255.255.252
Префікс мережі	/30
Адреса першого вузла	172.17.3.77
Адреса останнього вузла	172.17.3.78
Широкомовна адреса	172.17.3.79
Кількість вузлів мережі	2

Таблиця 3.9 – Маршрутизація R2 - MLSW1

З’єднання	R2 – MLSW1
Адреса мережі	172.17.3.80
Маска підмережі	255.255.255.252
Префікс мережі	/30
Адреса першого вузла	172.17.3.81
Адреса останнього вузла	172.17.3.82
Широкомовна адреса	172.17.3.83
Кількість вузлів мережі	2

Таблиця 3.10 – Маршрутизація R2 – MLSW2

З’єднання	R2 – MLSW2
Адреса мережі	172.17.3.84

Продовження таблиці 3.10

Маска підмережі	255.255.255.252
Префікс мережі	/30
Адреса першого вузла	172.17.3.85
Адреса останнього вузла	172.17.3.86
Широкомовна адреса	172.17.3.87
Кількість вузлів мережі	2

Таблиця маршрутизації між роутерами R1 та R2 з провайдером (таблиця 3.11- 3.12).

Таблиця 3.11 – Маршрутизація R1 - ISP

З'єднання	R1 – ISP
Адреса мережі	195.130.8.0
Маска підмережі	255.255.255.252
Префікс мережі	/30
Адреса першого вузла	195.130.8.1
Адреса останнього вузла	195.130.8.2
Широкомовна адреса	195.130.8.3
Кількість вузлів мережі	2

Таблиця 3.12 – Маршрутизація R2 - ISP

З'єднання	R2 – ISP
Адреса мережі	195.130.8.4
Маска підмережі	255.255.255.252
Префікс мережі	/30
Адреса першого вузла	195.130.8.5
Адреса останнього вузла	195.130.8.6
Широкомовна адреса	195.130.8.7
Кількість вузлів мережі	2

З урахуванням всіх необхідних вимог до мережі підприємства, розробимо її фізичну реалізацію в програмі cisco packet tracer. Почнемо з налаштування основних параметрів пристроїв, а саме імен хостів, вимкнення автоматичного пошуку домену, встановлення паролю на консолі та банерного повідомлення при спробі несанкціонованого підключення. Після налаштуємо інтерфейси, VLAN, протоколи маршрутизації та інші необхіді конфігурацій для забезпечення надійної та безпечної роботи мережі. Налаштування основних параметрів зображені на рисунку 3.1.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#hostname R2
R2(config)#line console 0
R2(config-line)#password 1234
R2(config-line)#login
R2(config-line)#exit
R2(config)#
R2(config)#enable password 1234
R2(config)#no ip domain lookup
R2(config)#banner motd #No Unauthorised Access!#
R2(config)#service password-encryption
R2(config)#
R2(config)#do wr
Building configuration...
[OK]
R2(config)#
R2(config)#ip domain name exima.net
R2(config)#username admin password 1234
R2(config)#crypto key generate rsa
The name for the keys will be: R2.exima.net
Choose the size of the key modulus in the range of 360 to 2048 for
your
  General Purpose Keys. Choosing a key modulus greater than 512 may
take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R2(config)#line vty 0 15
*Вер 1 0:45:2.775: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#
R2(config-line)#exit
R2(config)#
R2(config)#do wr
Building configuration...
[OK]
R2(config)#
R2(config)#
```

Рисунок 3.1 – Базові налаштування маршрутизатора R2

На рисунку 3.2 зображено оголошення портів, які з’єднують комутатор відділу продаж з MLSW1 та MLSW2, як магастральних.

```
Sales-SW(config)#interface range fa0/1-2
Sales-SW(config-if-range)#sw
Sales-SW(config-if-range)#switchport mo
Sales-SW(config-if-range)#switchport mode tr
Sales-SW(config-if-range)#switchport mode trunk


Sales-SW(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up

Sales-SW(config-if-range)#
Sales-SW(config-if-range)#
```

Рисунок 3.2 – Налаштування портів як магістральних

Створення vlan 10 та його налаштування (рисунок 3.3).

```
Sales-SW(config)#vlan 10
Sales-SW(config-vlan)#nam
Sales-SW(config-vlan)#name Sales
Sales-SW(config-vlan)#
Sales-SW(config-vlan)#
Sales-SW(config-vlan)#exit
Sales-SW(config)#int
Sales-SW(config)#interface ra
Sales-SW(config)#interface range fa0/3-24
Sales-SW(config-if-range)#swq
Sales-SW(config-if-range)#sw
Sales-SW(config-if-range)#switchport mod
Sales-SW(config-if-range)#switchport mode ac
Sales-SW(config-if-range)#switchport mode access
Sales-SW(config-if-range)#sw
Sales-SW(config-if-range)#switchport ac
Sales-SW(config-if-range)#switchport access vlan
Sales-SW(config-if-range)#switchport access vlan 10
Sales-SW(config-if-range)#exit
Sales-SW(config)#
```

Рисунок 3.3 – Створення vlan 10 та налаштування доступів на інтерфейсах до свіча і самої vlan 10

Виконаємо вимогу з налашування безпеки порту (рис 3.4) у відділі фінансів, а саме обмежити кількість пристроїв до 1, які можуть одночасно під’єднатися до порту комутатора. Використаємо липкий метод для отримання mac-адреси та відключення в режимі порушення.

```
Finance-SW(config)#
Finance-SW(config)#
Finance-SW(config)#int
Finance-SW(config)#interface ra
Finance-SW(config)#interface range fa0/3-24
Finance-SW(config-if-range)#sw
Finance-SW(config-if-range)#switchport po
Finance-SW(config-if-range)#switchport port-security ma
Finance-SW(config-if-range)#switchport port-security max
Finance-SW(config-if-range)#switchport port-security maximum 1
Finance-SW(config-if-range)#switchport port-security mac
Finance-SW(config-if-range)#switchport port-security mac-address st
Finance-SW(config-if-range)#switchport port-security mac-address sticky
Finance-SW(config-if-range)#sw
Finance-SW(config-if-range)#switchport po
Finance-SW(config-if-range)#switchport port-security v
Finance-SW(config-if-range)#switchport port-security violation sh
Finance-SW(config-if-range)#switchport port-security violation shutdown
Finance-SW(config-if-range)#exit
Finance-SW(config)#do wr
Building configuration...
[OK]
Finance-SW(config)#
```

Рисунок 3.4 – Налаштування безпеки порту комутатора у відділі фінансів

Налаштування протоколу OSPF на маршрутизаторах R1 (рисунок 3.5) та R2 (рисунок 3.6), а також на комутаторах MLSW1 (рисунок 3.7) та MLSW2 (рисунок 3.8) за допомогою консолі.

```
R1(config)#router ospf 10
R1(config-router)#router-id 3.3.3.3
R1(config-router)#
R1(config-router)#network 172.17.3.72 0.0.0.3 area 0
R1(config-router)#network 172.17.3.76 0.0.0.3 area 0
R1(config-router)#network 192.130.8.0 0.0.0.3 area 0
R1(config-router)#
R1(config-router)#do wr
Building configuration...
[OK]
R1(config-router)#ex
R1(config)#
```

Рисунок 3.5 – Налаштування протоколу OSPF на маршрутизаторі R1

```
R2(config)#
R2(config)#router ospf 10
R2(config-router)#router-id 4.4.4.4
R2(config-router)#
R2(config-router)#network 172.17.3.80 0.0.0.3 area 0
R2(config-router)#network 172.17.3.84 0.0.0.3 area 0
R2(config-router)#network 192.130.8.4 0.0.0.3 area 0
R2(config-router)#
R2(config-router)#do wr
Building configuration...
[OK]
R2(config-router)#ex
R2(config)#
```

Рисунок 3.6 – Налаштування протоколу OSPF на маршрутизаторі R2

```
Mlt-SW1(config)#ip routing
Mlt-SW1(config)#
Mlt-SW1(config)#router ospf 10
Mlt-SW1(config-router)#router-id 2.2.2.2
Mlt-SW1(config-router)#
Mlt-SW1(config-router)#network 172.17.1.0 0.0.0.63 are
% Incomplete command.
Mlt-SW1(config-router)#network 172.17.1.0 0.0.0.63 area 0
Mlt-SW1(config-router)#network 172.17.1.64 0.0.0.63 area 0
Mlt-SW1(config-router)#network 172.17.2.0 0.0.0.63 area 0
Mlt-SW1(config-router)#network 172.17.2.64 0.0.0.63 area 0
Mlt-SW1(config-router)#network 172.17.3.0 0.0.0.63 area 0
Mlt-SW1(config-router)#network 172.17.3.64 0.0.0.7 area 0
Mlt-SW1(config-router)#
Mlt-SW1(config-router)#network 172.17.3.72 0.0.0.3 area 0
Mlt-SW1(config-router)#network 172.17.3.80 0.0.0.3 area 0
Mlt-SW1(config-router)#
Mlt-SW1(config-router)#
Mlt-SW1(config-router)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Mlt-SW1(config-router)#
Mlt-SW1(config-router)#
Mlt-SW1(config-router)#
04:51:26: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on
GigabitEthernet1/0/1 from LOADING to FULL, Loading Done

04:52:40: %OSPF-5-ADJCHG: Process 10, Nbr 4.4.4.4 on
GigabitEthernet1/0/2 from LOADING to FULL, Loading Done

Mlt-SW1(config-router)#
```

Рисунок 3.7 – Налаштування протоколу OSPF на комутаторі MLSW1

```
Mlt-SW2(config)#ro
Mlt-SW2(config)#router os
Mlt-SW2(config)#router ospf 10
Mlt-SW2(config-router)#ne
Mlt-SW2(config-router)#net
Mlt-SW2(config-router)#network 172.17.1.0 0.0.0.63 are
Mlt-SW2(config-router)#network 172.17.1.0 0.0.0.63 area 0
Mlt-SW2(config-router)#network 172.17.1.64 0.0.0.63 area 0
Mlt-SW2(config-router)#network 172.17.2.0 0.0.0.63 area 0
Mlt-SW2(config-router)#network 172.17.2.64 0.0.0.63 area 0
Mlt-SW2(config-router)#network 172.17.3.0 0.0.0.63 area 0
Mlt-SW2(config-router)#network 172.17.3.64 0.0.0.7 area 0
Mlt-SW2(config-router)#
Mlt-SW2(config-router)#ne
Mlt-SW2(config-router)#networr
Mlt-SW2(config-router)#networr
Mlt-SW2(config-router)#networ
Mlt-SW2(config-router)#network 172.17.3.76 0.0.0.3 ar
Mlt-SW2(config-router)#network 172.17.3.76 0.0.0.3 area 0
Mlt-SW2(config-router)#network 172.17.3.84 0.0.0.3 area 0
Mlt-SW2(config-router)#ex
Mlt-SW2(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Mlt-SW2(config)#
Mlt-SW2(config)#
```

Рисунок 3.8 – Налаштування протоколу OSPF на комутаторі MLSW2

Налаштування DHCP з допомогою інтерфейсу обладнання зображено на рисунку 3.9.

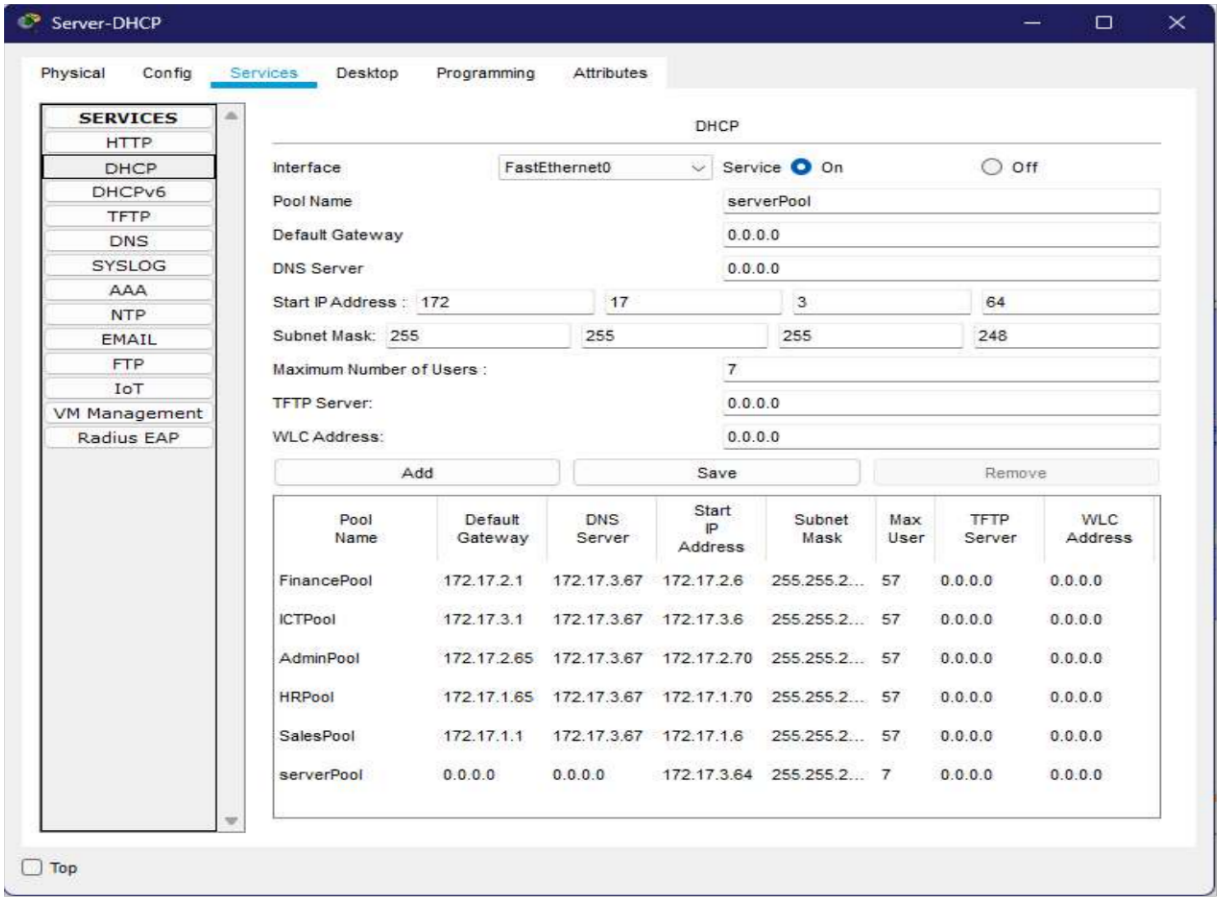

Рисунок 3.9 – Налаштування протоколу DHCP для кожного відділу

Налаштування NAT та списків контролю доступу на маршрутизаторах R2 (рисунок 3.10) та R1 (рисунок 3.11 та рисунок 3.12).

```
R2(config)#ip nat inside source list 1 interface se0/2/0 overload
R2(config)#
R2(config)#access-list 1 permit 172.17.1.0 0.0.0.63
R2(config)#access-list 1 permit 172.17.1.64 0.0.0.63
R2(config)#access-list 1 permit 172.17.2.0 0.0.0.63
R2(config)#access-list 1 permit 172.17.2.64 0.0.0.63
R2(config)#access-list 1 permit 172.17.3.0 0.0.0.63
R2(config)#access-list 1 permit 172.17.3.64 0.0.0.7
R2(config)#
R2(config)#
R2(config)#do wr
Building configuration...
[OK]
R2(config)#
R2(config)#
R2(config)#int ran
R2(config)#int range gig0/0-1
R2(config-if-range)#ip nat
R2(config-if-range)#ip nat in
R2(config-if-range)#ip nat inside
R2(config-if-range)#ex
R2(config)#
R2(config)#int se0/2/0
R2(config-if)#in
R2(config-if)#ip
R2(config-if)#ip na
R2(config-if)#ip nat ou
R2(config-if)#ip nat outside
R2(config-if)#
R2(config-if)#ex
R2(config)#do wr
Building configuration...
[OK]
R2(config)#
R2(config)#
```

Рисунок 3.10 – Налаштування NAT та списку контролю доступу на маршрутизаторі R2

```
R1(config)#int range gig0/0-1
R1(config-if-range)#ip nat
R1(config-if-range)#ip nat in
R1(config-if-range)#ip nat inside
R1(config-if-range)#ex
R1(config)#
R1(config)#
R1(config)#do wr
Building configuration...
[OK]
R1(config)#
R1(config)#
R1(config)#int se0/2/0
R1(config-if)#ip nat o
R1(config-if)#ip nat outside
R1(config-if)#ex
R1(config)#do wr
Building configuration...
[OK]
R1(config)#
R1(config)#
R1(config)#
```

Рисунок 3.11 – Налаштування NAT на маршрутизаторі R1

```
Rl(config)#ip nat inside source list 1 interface se0/2/0 overload
Rl(config)#
Rl(config)#
Rl(config)#
Rl(config)#
Rl(config)#ac
Rl(config)#access-list 1 pe
Rl(config)#access-list 1 permit 172.17.1.0 0.0.0.63
Rl(config)#access-list 1 permit 172.17.1.64 0.0.0.63
Rl(config)#access-list 1 permit 172.17.2.0 0.0.0.63
Rl(config)#access-list 1 permit 172.17.2.64 0.0.0.63
Rl(config)#access-list 1 permit 172.17.3.0 0.0.0.63
Rl(config)#access-list 1 permit 172.17.3.64 0.0.0.7
Rl(config)#
Rl(config)#
```

Рисунок 3.12 – Налаштування списку контролю доступу на маршрутизаторі R1

Виконаємо налаштування допоміжних адрес на комутаторах MLSW1 (рисунок 3.13) та MLSW2 (рисунок 3.14) для правильної обробки dhcp запитів.

```
Mlt-SWl(config)#
Mlt-SWl(config)#int vlan 10
Mlt-SWl(config-if)#no sh
Mlt-SWl(config-if)#ip add 172.17.1.1 255.255.255.192
Mlt-SWl(config-if)#
Mlt-SWl(config-if)#ip helper-address 172.17.3.66
Mlt-SWl(config-if)#ex
Mlt-SWl(config)#
Mlt-SWl(config)#int vlan 20
Mlt-SWl(config-if)#no sh
Mlt-SWl(config-if)#ip add 172.17.1.65 255.255.255.192
Mlt-SWl(config-if)#
Mlt-SWl(config-if)#ip helper-address 172.17.3.66
Mlt-SWl(config-if)#ex
Mlt-SWl(config)#
Mlt-SWl(config)#int vlan 30
Mlt-SWl(config-if)#no sh
Mlt-SWl(config-if)#ip add 172.17.2.1 255.255.255.192
Mlt-SWl(config-if)#
Mlt-SWl(config-if)#ip helper-address 172.17.3.66
Mlt-SWl(config-if)#ex
Mlt-SWl(config)#
Mlt-SWl(config)#int vlan 40
Mlt-SWl(config-if)#no sh
Mlt-SWl(config-if)#ip add 172.17.2.65 255.255.255.192
Mlt-SWl(config-if)#
Mlt-SWl(config-if)#ip helper-address 172.17.3.66
Mlt-SWl(config-if)#ex
Mlt-SWl(config)#
Mlt-SWl(config)#int vlan 50
Mlt-SWl(config-if)#no sh
Mlt-SWl(config-if)#ip add 172.17.3.1 255.255.255.192
Mlt-SWl(config-if)#
Mlt-SWl(config-if)#ip helper-address 172.17.3.66
Mlt-SWl(config-if)#ex
Mlt-SWl(config)#
Mlt-SWl(config)#int vlan 60
Mlt-SWl(config-if)#no sh
Mlt-SWl(config-if)#ip add 172.17.3.65 255.255.255.248
Mlt-SWl(config-if)#
Mlt-SWl(config-if)#ip helper-address 172.17.3.66
Mlt-SWl(config-if)#ex
Mlt-SWl(config)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
```

Рисунок 3.13 – Налаштування ip helper-address на MLSW1

```
Mlt-SW2(config)#int vlan 10
Mlt-SW2(config-if)#no sh
Mlt-SW2(config-if)#ip add 172.17.1.1 255.255.255.192
Mlt-SW2(config-if)#
Mlt-SW2(config-if)#ip helper-address 172.17.3.66
Mlt-SW2(config-if)#ex
Mlt-SW2(config)#
Mlt-SW2(config)#int vlan 20
Mlt-SW2(config-if)#no sh
Mlt-SW2(config-if)#ip add 172.17.1.65 255.255.255.192
Mlt-SW2(config-if)#
Mlt-SW2(config-if)#ip helper-address 172.17.3.66
Mlt-SW2(config-if)#ex
Mlt-SW2(config)#
Mlt-SW2(config)#int vlan 30
Mlt-SW2(config-if)#no sh
Mlt-SW2(config-if)#ip add 172.17.2.1 255.255.255.192
Mlt-SW2(config-if)#
Mlt-SW2(config-if)#ip helper-address 172.17.3.66
Mlt-SW2(config-if)#ex
Mlt-SW2(config)#
Mlt-SW2(config)#int vlan 40
Mlt-SW2(config-if)#no sh
Mlt-SW2(config-if)#ip add 172.17.2.65 255.255.255.192
Mlt-SW2(config-if)#
Mlt-SW2(config-if)#ip helper-address 172.17.3.66
Mlt-SW2(config-if)#ex
Mlt-SW2(config)#
Mlt-SW2(config)#int vlan 50
Mlt-SW2(config-if)#no sh
Mlt-SW2(config-if)#ip add 172.17.3.1 255.255.255.192
Mlt-SW2(config-if)#
Mlt-SW2(config-if)#ip helper-address 172.17.3.66
Mlt-SW2(config-if)#ex
Mlt-SW2(config)#
Mlt-SW2(config)#int vlan 60
Mlt-SW2(config-if)#no sh
Mlt-SW2(config-if)#ip add 172.17.3.65 255.255.255.248
Mlt-SW2(config-if)#
Mlt-SW2(config-if)#ip helper-address 172.17.3.66
Mlt-SW2(config-if)#ex
Mlt-SW2(config)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
```

Рисунок 3.14 – Налаштування ip helper-address на MLSW2

На рисунку 3.15 зображено топологію всієї мережі підприємства.

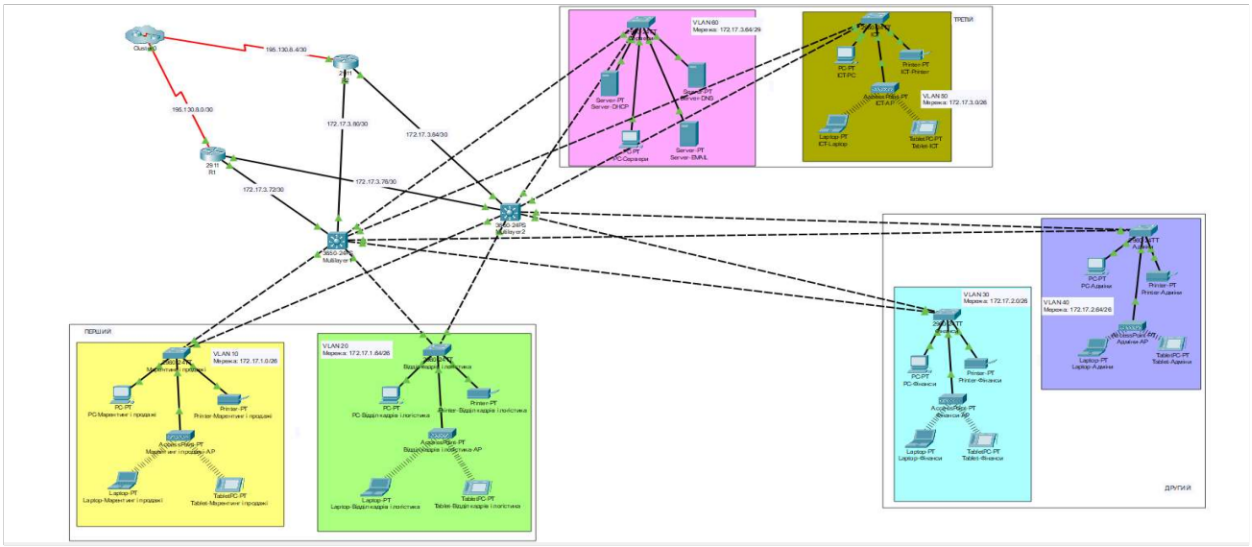

Рисунок 3.15 – Вигляд проекту мережі у cisco packet tracer

3.4 Апаратне забезпечення

Правильний вибір апаратного забезпечення є ключем до забезпечення ефективної роботи будь-якої інформаційної системи, а також для оптимізації витрат і підвищення продуктивності. Апаратне забезпечення має відповідати вимогам програмного забезпечення для того, щоб уникнути затримок при роботі. Також варто використовувати якісні компоненти, щоб зменшити ризик збоїв і простоїв системи.

Структура підприємства включає в себе 3 поверхи, на кожному з яких розташовується по 2 відділи. У кожному відділі знаходиться комутатор, 48 комп'ютерів, 8 принтерів та одна точка доступу. У серверній кімнаті знаходиться комутатор, 3 сервери та 3 комп'ютера.

Для відділів продаж, логістики, фінансів, адміністраторів та ІСТ обрано комутатор Cisco Catalyst 1200.

Основні характеристики Cisco Catalyst 1200 (рисунок 3.16):

– комутатор має 48 портів, які підтримують швидкість 10/100/1000 Мбіт/сек. Вони призначені для підключення різних пристроїв, таких як комп'ютери, сервери та інші мережеві пристрої;

– комутатор має 4 спеціальних порти SFP (Small Form-Factor Pluggable) для підключення до вищих рівнів мережі або інших комутаторів;

– даний комутатор може живити підключені пристрої через Ethernet-кабель за допомогою технології PoE+ (Power over Ethernet). Загальна потужність PoE становить до 740 Вт;

– комутатор немає вентиляторів, що робить його ідеальним для використання в офісних приміщеннях;

– розміри комутатора становлять приблизно 17,5 x 10,73 x 1,73 дюйма (ширина x глибина x висота);

– комутатор має RJ-45 порт для підключення консолі та USB-порти для зберігання даних та консолі через Bluetooth.

Рисунок 3.16 – Вигляд комутатора Cisco Catalyst 1200 [14]

Переваги:

– розширені можливості. Комутатор підтримує різні протоколи і функції, що дозволяє налаштовувати і оптимізувати роботу мережі згідно з потребами конкретного підприємства;

– безпека. Вбудовані механізми безпеки Cisco Catalyst 1200 забезпечать надійний захистити мережі від різноманітних загроз, що є важливим аспектом для будь-якої бізнес-мережі;

– сумісність з іншим обладнанням. Cisco Catalyst 1200 інтегрується з іншим обладнанням Cisco та іншими мережевими пристроями. Завдяки цьому можливо розробити рішення з високою сумісністю та взаємодією.

В серверну кімнату було обранрано комутатор Cisco C1000-8P-2G-L (рисунок 3.17). Основіні характеритики:

– має 8 портів Ethernet які підримують швидкість 10/100/1000 Мбіт/сек., що дозволяє підключити до мережі різні пристрої з різними швидкостями передачі даних;

– крім Ethernet-портів, комутатор має 2 спеціальних порти SFP (Small Form-Factor Pluggable) для підключення до вищих рівнів мережі або інших комутаторів;

– комутатор має можливість живлення пристроїв через Ethernet (PoE) на 8 портах, що дозволяє живити бездротові точки доступу безпосередньо через мережу;

– комутатором можна керувати через консольний інтерфейс, веб-інтерфейс або з використанням протоколів управління мережею.

Рисунок 3.17 – Зовнішній вигляд Cisco C1000-8P-2G-L [13]

Модель точок доступу обрано Cisco CBW240AC-E (рисунок 3.18). ЇЇ характеристики:

– CBW240AC-E підтримує стандарти Wi-Fi 802.11ac Wave 2, які забезпечують високу швидкість передачі даних та стабільність зв’язку підключених пристроїв;

– функція MU-MIMO дозволяє точці доступу обслуговувати багато пристроїв одночасно, що оптимізує використання бездротового каналу та підвищує ефективність мережі;

– CBW240AC-E може живитися через Ethernet-кабель. Це дозволяє спростити процес встановлення та дозволяє розмістити точку доступу де буде зручно;

– точка доступу використовує сучасні механізми безпеки, такі як WPA/WPA2, аутентифікацію на основі 802.1X, фільтрацію MAC-адрес, що забезпечує захист мережі та даних користувачів;

– є можливість керувати точкою через хмарне програмне забезпечення Cisco Meraki. Дана функція дозволяє адміністраторам моніторити та керувати мережею з будь-якої точки, де є доступ до Інтернету;

– за допомогою технології Beamforming точка доступу може автоматично налаштовувати напрямок передачі сигналу, щоб забезпечити оптимальну швидкість та стабільність зв’язку для кожного пристрою.

Рисунок 3.18 – Зовнішній вигляд Cisco CBW240AC-E [16]

Модель принтера HP Color LaserJet Enterprise MFP M480f (рисунок 3.19) та її характеристики:

– швидкість друку до 27 стор./хв (ч/б і кольоровий);

– роздільна здатність друку до 600 x 600 dpi;

– функції. Друк, копіювання, сканування, факс;

– ємність подачі паперу 300 аркушів (250-аркушовий основний лоток, 100-аркушовий багатоцільовий лоток);

– автоматичний двосторонній друк;

– двостороннє сканування, оптична роздільна здатність до 1200 x 1200 dpi;

– підключення Gigabit Ethernet, USB 2.0, хост-USB;

– функції безпеки. HP Sure Start, Whitelisting, шифрування даних, автентифікація користувачів.

Рисунок 3.19 – Зовнішній вигляд HP Color LaserJet Enterprise MFP M480f [19]

Як персональний комп’ютер обрано моноблок ASUS A3402 (рисунок 3.20). Його характеристики:

– процесор Intel Core i7-1255U;

– дисплей 23.8 full hd (1920 x 1080);

– озп 16 гб DDR4;

– зберігання 1 тб ssd;

– графіка Intel Iris Xe;

– ос Windows 11;

– порти 4 x USB 3.2 Gen 1 Type-A, 1 x USB 3.2 Gen 1 Type-C, HDMI, Ethernet, 3.5 мм аудіо, картрідер;

– бездротові технології Wi-Fi 6(802.11ax), Bluetooth 5.0;

– звук. Вбудовані стереодинаміки з ASUS SonicMaster.

Даний моноблок має потужний процесору, відмінний дисплей з вузькими рамками і чудовою передачею кольорів, великий об’єм оперативною пам’яті забезпечить комфортну роботу. Також він має регульовану підставка,що роблять його ідеальним для будь-якого робочого місця.

Рисунок 3.20 – Зовнішній вигляд ASUS A3402 [11]

Багаторівневим комутатором виступає Cisco Catalyst 2960-LP (рисунок 3.21). Його характеристики:

– 16 портів 10/100/1000 Мбіт/сек Ethernet для підключення різних пристроїв;

– є додаткові 2 порти SFP які використовують для підключення до вищих рівнів мережі або інших комутаторів;

– комутатор підтримує (PoE), що дає можливість живити пристрої через Ethernet, такі як IP-телефони чи бездротові точки доступу;

– комутатором можна керувати через консольний порт, веб-інтерфейс або з використанням протоколів управління мережею;

– підтримує протоколи безпеки 802.1X, що дозволяє аутентифікувати пристрої, які підключаються до мережі, перед наданням доступу до ресурсів;

– функція MAC Address Notification сповіщає адміністратора про зміну MAC-адреси на порті комутатора, що дозволяє передбачити несанкціонований доступ;

– комутатор має підтримку VLAN, QoS, IPv6, захист від DoS-атак.

Рисунок 3.21 – Зовнішній вигляд Cisco Catalyst 2960-LP [15]

Маршрутизатори обрано Cisco ISR4331 (рисунок 3.22). Характеристики:

– маршрутизатор має максимальну пропускну здатність до 100 Мбіт/секунду;

– маршрутизатор має вбудовані слоти для розширень, що дозволяє розширити його функціональність;

– має вбудовані порти Gigabit Ethernet для LAN та WAN підключень;

– наявні вбудовані засоби захисту мережі, а саме фірмовий захист від атак, захист від вторгнень та захист від атак типу DOS;

– маршрутизатор підтримує VPN, що дозволяє зробити безпечний тунель зв’язку між віддаленими мережами або забезпечити безпечний доступу до корпоративних ресурсів;

–можливість управління за допомогою консольного інтерфейсу, веб-інтерфейс та протоколів управління мережею, такого як SNMP.

Рисунок 3.22 – Зовнішній вигляд Cisco ISR4331 [17]

Сервери в серверній кімнаті Cisco Blade Server B200 M4 (рисунок 3.23).

Рисунок 3.23 – Зовнішній вигляд Cisco Blade Server B200 M4 [12]

Характеристики:

– процессоры 2x Intel Xeon E5-2683 v3 (2 ГГц, 14 ядер);

– оперативная память 64 ГБ DDR4 ECC Registered DIMM;

– зберігання даних. Підтримка HDD/SSD 2.5 до 3,2 ТБ. контролери: SAS або SATA;

– мережевий адаптер Cisco VIC1340 з підтримкою Ethernet, FCoE;

– форм фактор модульний сервер, призначений для встановлення в шасі Blade від Cisco UCS (Unified Computing System). Така структура дозволить легко розширити ресурси сервера за потреби та дозволяє керувати ресурсами через єдину систему управління;

– Cisco Blade Server B200 M4 сумісний з різними версіями Windows Server, різними дистрибутиви Linux та платформою віртуалізації VMware vSphere, що дозволяє вибрати оптимальну операційну систему для різних робочих навантажень та додатків.

ВИСНОВКИ

В цій кваліфікаційній роботі було проведено дослідження та розробку проекту локальної комп'ютерної мережі підприємства. Робота складається з трьох розділів, в кожному з яких висвітлено певні аспекти комп'ютерних мереж.

У першому розділі були розглянуті основні терміни і поняття, які відіграють важливу роль у розумінні комп'ютерних мереж. У другому розділі було описано програмні засоби які були застовсовані при розробці. У третьому розділі описано процес розробки комп'ютерної мережі.

Виконані завдання:

– розроблено проект комп'ютерної мережі для підприємства. Для побудо ви мережі було обрано гібридну топологію, яка поєднує елементи зіркової та ієрархічної топологій. Для забезпечення оптимальної роботи мережі було виб рано відповідне мережеве обладнання. Комутатори Cisco Catalyst 1200, маршрутизатори Cisco ISR4331, точки доступу Cisco CBW240AC-E, сервери Cisco Blade Server B200 M4.

– проведено аналіз та вибір найкращих протоколів маршрутизації та комутації. Для маршрутизації використовується протокол OSPF, який забезпечує ефективну комунікацію між пристроями та надійність. Для комутації застосо вуються протоколи STP та RSTP, що запобігають утворенню петель і забезпечують відмовостійкість мережі;

– налаштовано мережеві пристрої, зокрема маршрутизатори та комутато ри. Всі пристрої в мережі динамічно отримають IP-адресу від виділеного сервера DHCP. На маршрутизаторах налаштовано протоколи маршрутизації, імена хостів, пароль консолі, банерні повідомлення, вимкнено пошук домену IP, а на комутаторах – налаштовано VLAN та протоколи комутації;

– впроваджено засоби безпеки. Налаштовано доступ до мережевих ресур сів через списки контролю доступу (ACL). Було визначено правила доступу для різних підмереж, що дозволяє ефективно захистити дані та забезпечити безпеку мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вишняков, В. М. Принципи побудови комп’ютерних мереж: навч. посіб. В. М. Вишняков. Київ: КНУБА, 2022. 124 с.

2. Жураковський, Б. Ю., Зенів, І. О. Комп’ютерні мережі. Частина 2: навч. посіб. Б. Ю. Жураковський, І. О. Зенів. Київ: Київський університет, 2020. 372 с.

3. Модель OSI. URL: https://uk.wikipedia.org/wiki/Мережева_модель_OSI (дата звернення 23.12.23).

4. Сервери. URL: https://www.cisco.com/site/us/en/products/computing/ servers-unifiedcomputin gsystems/index.html (дата звернення 27.12.23).

5. Топологія Дерево. URL: https://mark-techno.kz/novosti/item/298 (дата звернення 04.01.24).

6. Топологія Зірка. URL: https://uk.wikipedia.org/wiki/Зірка_(топологія) (дата звернення 05.01.24).

7. Топологія Меш. URL: https://www.education.ua/blog/15772 (дата звернення 03.01.24).

8. Топологія Кільце. URL: https://uk.wikipedia.org/wiki/Кільцева_ топологія_мережі (дата звернення 05.01.24).

9. Топологія Шина. URL: https://vseosvita.ua/lesson/vydy-topolohii-341873.html (дата звернення 06.01.24);

10. Точки Доступу. URL: https://www.cisco.com/site/us/en/products/ networking/wireless/accesspoints/index.html (дата звернення 10.05.24).

11. ASUS A3402. URL: https://www.asus.com/ua-ua/displays-desktops/all-in-one-pcs/all-series/asus-a3402/ (дата звернення 15.05.24).

12. Cisco Blade Server B200 M4. ULR https://systemsolutions.com.ua/ content/cisco-ucs-b200-m4 (дата звернення 15.05.24).

13. Cisco C1000-8P-2G-L. ULR: https://comtrade.ua/ua/cisco-c1000-8p-2g-l/ (дата звернення 11.05.24).

14. Cisco Catalyst 1200. URL: https://comtrade.ua/ua/cisco-catalyst-1200-c1200-48t-4g/ (дата звернення 12.05.24).

15. Cisco Catalyst 2960-LP. URL: https://stack-systems.com.ua/kommutator-cisco-ws-c2960l-16ps-ll (дата звернення 12.05.24).

16. Cisco CBW240AC-E. URL: https://comtrade.ua/ua/cisco-cbw240ac-e/ (дата звернення 13.05.24).

17. Cisco ISR4331. URL: https://stack-systems.com.ua/marshrutizator-cisco-isr4331-k9 (дата звернення 14.05.24).

18. Cisco Networking Academy. Introduction to Networks Companion Guide. - 1st ed. - Pearson, 2020. ISBN-13: 978-0-13-663366-2. 750 с.

19. HP Color LaserJet Enterprise MFP M480f. URL:-https://www.hp.com/ua-uk/products/printers/product-details/2101097035 (дата звернення 09.05.24).